Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2016 Proceedings

International Conference on Information Resources Management (CONF-IRM)

2016

Measuring The Organizational Impact of Security Breaches: Patterns of Factors and Correlates

Kevin P. Gallagher
Cleveland State University, k.gallagher96@csuohio.edu

Xiaoni Zhang
Northern Kentucky University, zhangx@nku.edu

Vickie Coleman Gallagher
Cleveland State University, v.c.gallagher@csuohio.edu

43. Measuring The Organizational Impact of Security Breaches: Patterns of Factors and Correlates

Kevin P. Gallagher
Cleveland State University
k.gallagher96@csuohio.edu

Xiaoni Zhang
Northern Kentucky University
Zhangx@nku.edu

Vickie Coleman Gallagher
Cleveland State University
v.c.gallagher@csuohio.edu

Abstract
As the use of technology permeates organizations, as well as our personal and professional lives, organizational research has aimed to report the incidence of security breaches. However, self-reporting in survey research is flawed given that organizations are hesitant to admit to loss of sensitive data and other security breaches. Furthermore, there are gradients of breaches, rather than binomial occurrences, or lack of occurrences. Hence, a more comprehensive and less obtrusive measure of the nature and impact of breaches is necessary in order to advance theory and practice. As such, we tested a new measure of impact with representatives from over 500 organizations intended to measure the extent of a breach and its subsequent impact on the organization. We developed the construct using exploratory and confirmatory factor analysis and report on convergent validity. We find the impact of breaches tends to be greater for decentralized organizations, smaller organizations, and those within the financial services industry.

Keywords
IT Security, Impact of Security Breaches, Organizational Impacts, Measurement, Dependent Variable

1. Introduction
Security breaches in organizations are a systemic concern in the US and around the globe. Recent US governmental policies and public disclosure laws have required companies to report security breaches. As such, many studies have reported the occurrence and types of breaches, or, the effectiveness of preventative and deterrence measures (Keller et al., 2008, Price-Waterhouse Coopers 2008, Richardson 2008 & 2010, Herath & Rao 2009). Others have sought to understand the impact of these public announcements and the breaches themselves, such as decreases in market value (Goel & Shawky, 2009) and impacts on the stock market (Garg, Curtis & Harper, 2003). Finally, niche markets have explored how security breaches impact hotel guest perceptions (Berezina, Cobanoglu, Miller & Kwansa, 2012) and supply chain performance (Sindhuja, 2014). However, the utility of such reporting in academic research (as well as the measures used in extant research) is suspect, given that companies are often hesitant to report breaches in a survey research format. In fact, the CSI Survey (Richardson, 2008, 2010) reported that many respondents were unwilling to report actual incidents, hindering academic research into this area. In fact, Richardson states that "fewer respondents than ever are willing to share specific information about the dollar

losses they incurred" (2010). Garg and colleagues (2003) highlighted studies showing breaches to be anywhere from 36% of companies to 90% of companies experiencing breaches (illustrating hesitancy in reporting depending on the surveyor). To further complicate matters, breaches can go undetected for some time, as exemplified by the well publicized breach at TJX. (For an in-depth case study analysis of this event, the effect on the company, stakeholders, and effects over time, see Hovav & Gray, 2014.)

Rather than study the occurrence of breaches or safeguards implemented, the current research explores a new measure of the impact that security breaches have on the organization. The severity of security breaches is therefore based on the actual degree of impact on the organization and its operations, rather than an explicit reporting of the type of breach, or the distal market conditions that may surround a public disclosure of a breach (Goel & Shawky, 2009). In fact, some researchers would argue that the effect of security incidents on the market value of companies have shown mixed results (Hovav & Gray, 2014). As such, we argue, with our new measure, that breaches can impact an organization not only through loss of revenue but by damaging its reputation, by rendered its systems inoperable, causing lower morale, and wasting the time of its personnel. Hence, regardless of the reason for the breach, we argue that the impact is of greater importance to advancing theory.

In order to explore the impact of IT security breaches, we adapt an existing set of questions from a measure of business crime impact (Elliott, 2008). We tested the construct with data from over 500 organizations, surveying key informants from the institutions. We developed the construct using exploratory and confirmatory factor analysis and report on convergent validity. First we provide a background with regard to the motivation and objectives of the study, a literature review that justifies the need for this study, selection of measurement items, and development of our hypotheses. Subsequent sections outline the method, analysis, results, and discussion, which include the study's contributions, limitations, and opportunities for future research.

2. Literature Review & Hypothesis Development

As noted above, the cause and types of security breaches has been studied (or attempts have been made); yet there exists a disconnect between our understanding of these breaches and the relevant outcomes. The objective of this study was to understand the impact of IT security breaches in organizations, both large and small, across a variety of industry sectors. In reviewing the academic literature on IT security we were unable to find an existing measure of impact. Therefore, our objective is to inform academic research through the development and application of a measure of impact. Future research will then better inform theory and practice as to the relationship between breaches, preventative measures, and other organizational or institutional factors.

Our research also aims to inform organizational practice and governmental policy by describing the differences in impact found across a variety of organizations, such as degree of centralization, size of organization, and industry. Executives and policy makers are concerned with the degree to which security breaches impact organizations, given the implications in a variety of domains (e.g., reputation, profits, consumer confidence, etc.). Thus, the funding for the study was in part provided by a grant from the National Institute for Justice of the U.S. Department of Justice. This funding enabled us to collect data from a very large sample of over 500 organizations from across the United States.

2.1 Need to Measure the Impact of Security Breaches

Academic study of IT security has grown recently, as the increasingly ubiquitous use of internet-related technologies has become critical to the operation of most modern organizations. Yet IS academic research in this area is still in its infancy (Zafar & Clark, 2009). As is often the case, the focus on the technology related to security has outpaced the focus on management of the technology in both academic research, as well as in practice.

As noted earlier, self-report studies that ask organizations to report the nature and occurrence of breaches is likely to be flawed. Employees often underestimate the frequency of security breaches (Herath & Rao 2009) and organizations have little if no incentive to make security breaches public (Zafar & Clark, 2009). One logical reason for not reporting incidents is the fear that public disclosure of incidents will impact the reputation of the organization (Cavusoglu et al., 2004). While empirical evidence suggests there is a limited overall negative market reaction to public announcements, there is a highly significant reaction to certain types of breaches (Campbell, Gordon, Loeb & Zhou, 2003), with confidential data having a higher impact on the stock market. This pattern of underestimating and/or underreporting the occurrence breaches makes it difficult evaluate preventative efforts, as well as management practices that can mitigate the consequences of breaches.

Aside from adherence to regulatory rules, overall there are few incentives for organizations to report incidents, leaving it difficult for academic studies to assess the design and efficacy of the security policies and technologies adopted to prevent or respond to breaches. Hence, while studies reporting the frequency of different types of breaches are important to raise awareness, these reported occurrences cannot always be considered reliable, nor can they easily be correlated with the impact on the organization internally (beyond external public relations). We therefore believe that real advances can be achieved by having a measure to assess the severity of the impact of incidents. This will enable research to better evaluate the value of different safeguards and to understand the effectiveness of policies, procedures and technologies.

2.2 Prior Research on Impact

Given that there is a lack of research in the area of outcomes (or independent variables) related to breaches, we chose to expand our search to other domains. We identified a business crime survey (Elliott, 2008) that measured the impact of crime, although some of the items (e.g., moved premises, changed layout design) seemed less relevant to our objectives than others. Ultimately six of the items were retained and are bolded in the text below, and respondents were asked to report on these items on a 1 to 7 scale, with 1 representing “no impact” and 7 representing “significant impact”. Our paper proceeds with the rationale for their retention, thus formulating the construct proposed in this paper.

First, losses are often incurred during a response to breaches, which results in employees spending time that detracts from their overall productivity, resulting in a relative waste of that employee’s time. Thus, we determined that the impact construct should include items to measure **disruption to operations**, **staff downtime** and the impact that a breach may have on **lowering company moral.**

Second, markets may react to breaches, having an impact on the organization's relationship with its customers. Thus, there is the potential negative implication that a breach could have on revenues (Campbell et al., 2003). For example, Amazon experienced a denial of service attack that resulted in millions of dollars in lost business. In this instance, the frequency of such attacks is arguably less meaningful than the fact that a single significant attack occurred. Therefore we believe that in developing a construct for impact we should include an item that measures **loss of revenue**.

In addition to the impact breaches may have on an organization's revenue and operations, the impact of breaches may also have other financial consequences. As with the single occurrence of a breach, organization respondents are often unwilling to report the dollar figure associated with an incident. However, secondary costs may not be as sensitive an issue, such as the cost of insurance secured to protect the company from losses. Breaches may also be viewed as a risk by insurance companies, whose reaction to an incident could be to raise premiums. Therefore the impact construct needs to measure **increases in insurance costs**.

Prior survey research reported that 80% of respondents acknowledged financial losses related to computer crimes, although 44% were unwilling to quantify those losses, again reinforcing the argument that impact to reputation is a vital concern which translates into an unwillingness for managers to readily report on their occurrence (Gordon et al., 2005). Hence, we argue that the impact construct should include an item to measure **damage to company image**.

2.3 Hypothesis development and criterion validity

As in any effort to thwart criminal activity, it is important to understand and properly assess the levels of risk exposure in different areas (Dimopoulos et al., 2004). Prior studies have reported differences in the level of investment and efforts undertaken by organizations of different sizes and across different industry sectors (Dimopoulos et al., 2004). For example, organization size is related to likelihood of conducting a risk assessment (UK National Computing Center 2000). Risk assessments are linked to greater acceptance of security measures by employees and help to insure compliance (Rees & Allen, 2008). One of the main reasons smaller organizations do not conduct risk assessments are fears of disruptions to operations (Federal Aviation Association 2001).

Another reason for differences across organizations is that there are generally greater resources and larger IT staffs available in larger organizations (Straub, 1990; Blakely, 2002). The staff in smaller organizations may also have less knowledge of security solutions and less knowledge of how to approach the issue (Brake, 2002). Management in smaller organizations may also know employees well enough to become more trusting. The absence of accepted industry wide measures to enable the evaluation of the efforts of smaller and medium organizations may also be responsible for fewer assessments being conducted within smaller organizations (Robins, 2001).

Dimopoulos and colleagues published results of a study of small to medium size organizations where data was collected in UK and US to evaluate organizational attitudes toward security (2004). The study reports that large organizations (greater than 500 FTEs) were 21% more likely to be attending to the implementation of security safeguards than smaller organizations. Larger organizations have a budget dedicated to security (compared to just 15% of smaller organizations) and larger organizations have access to IT security experts. This lack of expertise may also explain why smaller organizations were also less likely to have a documented security policy.

Kankanhalli et al. (2003) also found that smaller organizations were engaged in fewer efforts focused on deterrence of security threats and that the deterrent efforts increased the effectiveness of IS security. However, larger organizations have more to lose. It is precisely their vulnerability that requires them to invest more heavily in assessments and the development of protocols. This may indeed reduce the sheer number of breaches, yet it may not minimize the impact. Hence, we hypothesize the following:

> **H1:** Larger organizations will experience greater impact (damages to reputation, disruptions to operations, etc.) from security breaches than smaller organizations.

Industry has received too little attention in information systems research and theory, and research has historically focused on too narrow a range of industries (Chiasson & Davidson, 2005). As such, we sought to incorporate industry into our model of interpreting how industry sector is related to security breaches. For example, the concern for security breaches is greater among organizations in the financial sector, due to the large potential impact that a breach could have on them (Goodhue & Straub, 1991). As such, it is logical that organizations in the financial sectors invest more in deterrent efforts (Kankanhalli, et al., 2003). Kankanhalli and colleagues also found that organizations in non-financial industry sectors invested less in deterrent efforts and subsequently were less effective at IS security. Organizations will experience greater impact, particularly when the types of breaches are more likely to be associated with sensitive data. That is, some industry sectors will also have a greater concern for IS security due to the impact it could have on their reputation (Goodhue & Straub, 1991). We therefore hypothesize that financial services, while they may indeed invest more in security initiatives, it is for good reason: financial services industry participants will report greater impact from security breaches.

> **H2:** Organizations in financial services industries will report greater impact from security breaches than non-financial services industry companies.

A great deal of prior research on IT organizational structure does exist, much of it focusing on the question of centralizing or decentralizing the IT function within an organization (King 1983, Sambamurthy and Zmud 1999). This approach informs questions of how best to manage the locus of decision-making and associated governance of IT (Brown and Magill 1994, 1998; and Sambamurthy and Zmud 1999). The structural approach also informs how organizations can manage the complex integration of systems, including their protection from breaches and organization of responses to incidents. To date, little research has documented how such structures might result in lowering or increasing the impact of security breaches.

The choice of management structures can ultimately hold implications for managing IT, given the increased complexity involved in the coordination, implementation and maintenance of security policies, technologies, and response plans and procedures that occur with greater decentralization. Thus, the benefits associated with greater centralization of structures should decrease the organization's impact from security breach incidents.

> **H3:** Centralized organizations will experience lower impact than decentralized organization.

3. Method

3.1 Sample and Data Collection

Development of the impact construct was conducted as a part of a larger study of the state of IT security. Our approach to investigating the state of IT security was to conduct both local and nation-wide online surveys. Initial surveys were pre-tested with local and regional key constituents of the university; however, the majority of the survey data were collected from individuals in over 500 organizations using existing survey panel members solicited through a research vendor. The panel was screened to identify lists of participants who fit a number of requirements, including a mix of demographics such as region, industry, etc. Next, their participation was requested through an email invitation. In order to insure that our participants were qualified to respond to the questions in the survey we used several forms of screening and validation. First, the survey panel was mined for respondents who were decision makers, had knowledge of IT and were managers in their organizations. Secondly, we asked respondents a series of screener questions about requisite knowledge of information technology and security issues within their company (e.g., policies, procedures, and management of IT). Third, we examined the survey responses (after data was collected) to insure that each screener response was reasonable given the size, industry and title of respondent. The sample analyzed in this report consists of 556 responses in a wide range of industries across the country. However, sample sizes vary based on the analysis (as noted below) and based on completeness of the data for a particular variable.

3.2 Analysis

We split the data randomly into two sets: one for exploratory factory analysis and the other for confirmatory analysis. AMOS 21 was used for the confirmatory analysis on the factor – policy assimilation and SPSS 22 was used to perform the hypotheses testing. Table 1 shows the frequency distribution of responses by industry.

Industry	**Percent**
Financial Services (Banking, Investment Serv., Insurance)	11.09%
Manufacturing (Mfg., Phara. /Chemical, Transport. /Distrib.)	17.14%
Education	10.08%
Professional Services (Consulting)	9.88%
Government	6.45%
Healthcare	9.27%
IT Products & Services (Software, Technology, Telecomm.)	11.29%
Retail and Real Estate (Property & Construction)	10.48%
Non-Profit Organizations	5.24%

Table 1: Distribution by Industry

Table 2 shows the exploratory factor analysis (n=232) with varimax rotation. The results show that the KMO is 0.88. The KMO measures the sampling adequacy which should be greater than 0.6 for a satisfactory factor analysis to proceed. Large values for the KMO measure indicate that a factor analysis of the variables is suitable. Two factors clearly emerge and items load on the construct they are supposed to load. The loadings in table 2 are in the range of 0.81 and 0.92, greater than

the suggested value of 0.5 (Straub, 1989).

Impact Measure	Mean	Std. Deviation	Loadings
Staff down-time	3.63	1.93	0.83
Disrupted operations	3.78	2.00	0.85
Lowered staff morale	3.29	2.05	0.92
Increased insurance costs	3.12	2.08	0.91
Lost business	3.10	2.09	0.92
Damaged company image	3.16	2.09	0.90

Table 2: Factor Loadings and Descriptive Statistics

Reliability/internal consistency measures the degree that the measurement items that reflect the same latent variable are in agreement with one another (Churchill, 1979). The most widely used internal consistency reliability coefficient is Cronbach's coefficient alpha (Cronbach, 1971). Some suggest the acceptance level for coefficient alpha should be at least 0.7 (Robinson et al., 1991). Our SPSS analysis shows that the Cronbach's alpha is 0.95 for impact.

Table 2 shows the descriptive statistics for the items of impact. When assessing the measurement model for impact, CFI=0.95, GFI =0.91 and AGFI=0.88 fit statistics were used. These indices indicate good model fit and provide evidence of both convergent validity and unidimensionality (Gerbing & Anderson, 1988; Bagozzi et al., 1991). In addition, as shown in Table 2 high and significant factor loadings provides further evidence of convergent validity. Table 3 shows the mean score of impact based on company size. As shown the company size with 500 or more has the highest mean of impact.

Company Size	N	Mean	Std. Deviation
Under 100	114	3.01	1.75
100 to 249	88	3.08	1.75
250 to 499	78	3.24	1.78
500 or More	173	3.92	1.76

Table 3: The Mean of Impact Based on Company size

Table 4 below shows that the results of ANOVA analysis. As shown, large companies (500 or more) are significantly different from the other three groups (under 100, 100-249, 250-499), supporting Hypothesis 1.

(I) Company Size	(J) Company Size	Mean Difference (I-J)	Std. Error	Sig.
500 or More	Under 100	.90741*	0.21	0
	100 to 249	.83664*	0.23	0
	250 to 499	.67260*	0.24	0.03

Table 4: ANOVA Results on Company Size

Table 5 shows the means of impact score based on different industries. The mean of financial services is the third highest. In partial support of Hypothesis 2, Table 6 shows that the mean score of impact for the financial services industry is only significantly different for three of the eight

other industry groups: professional services, government and non-profit organizations.

Industry	N	Mean	Std. Deviation
IT Products & Services (Software, Technology, Telecomm.)	56	4.11	1.73
Education	50	4.01	1.82
Financial Services (Banking, Investment Serv., Insurance)	55	3.95	1.73
Healthcare	46	3.64	1.97
Manufacturing (Mfg., Phara. /Chemical, Transport. /Distrib.)	85	3.39	1.77
Retail and Real Estate (Property & Construction)	52	3.00	1.74
Professional Services (Consulting)	49	2.76	1.57
Government	32	2.53	1.49
Non-Profit Organizations	26	2.48	1.51

Table 5: The Means of Impact Based on Industry Category

Industry	Industry	Mean Difference	Std. Error	Sig.
Financial Services (Banking, Investment Serv., Insurance)	Professional Services (Consulting)	1.19490*	.32	.01
	Government	1.41875*	.35	.00
	Non-Profit Organizations	1.46923*	.38	.01

Table 6. ANOVA Results of Impact on Industry Category

IT organization structure was measured using a scale variable ranging 1 through 9 with 1 indicating very centralized and 9 referring to very decentralized. To test H3, we split data into two categories: centralized and decentralized. To examine if there is a significant difference on impact between centralized and decentralized IT organization structure, t test was performed and Table 7 below shows the result. The centralized IT structure has a mean of 2.61 on impact and the decentralized organization has a mean of 3.30. The difference on impact between IT organization structure is significant at 1% level

Degree of Centralization (1-9) Mean Split	Mean	Std. Deviation	Std. Error Mean	
Centralized	2.61	1.78	0.18	P=1%
Decentralized	3.30	1.71	0.59	

Table 7: t Test between centralized and decentralized

4. Discussion and Conclusion

The motivation and objective of this paper was to establish a measure of the impact of security breaches and to assess differences in the impact experienced across organizations of different sizes, different industries, and the degree to which they are centralized or decentralized. Although organizational research has tested the incidence of breaches, experts agree that this method of analyzing outcomes is flawed such that organizations are hesitant to admit to breaches, particularly when the types of breaches include loss of sensitive data. A more comprehensive and less sensitive outcome measure is necessary in order to advance theory and practice. Therefore, based on prior research, we hypothesized that the impact of breaches will be greater for larger organizations, decentralized, and those within the financial services industry. Although larger organizations and those in financial services may indeed have more resources to dedicate to IT security, they also

have the most to lose. As expected, centralized organizations may have a better control over the management practices and protocols, hence experiencing lower impact from breaches.

Interestingly, financial services organizations have significantly different means compared to non-profits and professional service organizations. One explanation is perhaps that these institutions are not as desirable of a target to those who may wish to breach IT systems. An alternative explanation is that the latter lack the resources to adequately monitor and determine risk, and are subsequently unaware of the potential harm that may be caused to their operations, reputation, and insurance costs. Alternatively, government organizations are required to have policies and procedures, which should include monitoring of their systems. It may be that the representatives of these organizations in our sample set do not believe that breaches will impact them in the same manner—e.g., reputation is not as proximal a concept to government agencies, and insurance costs are not relevant.

Financial services industries have similar mean impact scores relative to health care, IT related services industries, and education. Considering the nature of the information maintained by educators and health care institutions, this finding makes intuitive sense. And, IT organizations clearly have insights into the magnitude of potential impacts. However, future research should explore the "why" of these phenomena, helping to inform the reasons for these similarities and differences in the data. For example, research has shown that learning over time can help to mitigate risk over time (Slayton, 2015), and, top management participation and organizational culture play key roles in encouraging employee compliance in information security policies (Hu, Dinev, Hart, & Cooke, 2012).

Our research, despite its contributions, is not without limitations. Our data is collected primarily via a panel of participants, not a random national sample. Furthermore, items to develop our measure were drawn from existing measures, based on theory and prior empirical evidence, not derived from grounded theory. Our initial analysis in this study relies on relatively simple statistics, and more sophisticated analysis is required. In our efforts to provide a new measure of impact, we were unable to provide predictive validity nor criterion related validity of other concepts as it related to antecedents. For example, variables that measure investment in safeguards, availability of resources, and organizational commitment to security efforts would be expected to predict degree of impact.

Future research is necessary to expand upon this analysis. Further testing of this measure will enable researchers to test relationships with antecedent variables such as specific security breaches, specific safeguards, or the implementation of a variety of management policies. Researcher should consider models and relationships controlling for the variables identified in this analysis. An established measure of the impact of breaches can also enable analysis of a breach's relationship to short-term or long-term performance of a firm or to the initiation of future actions the organization may undertake. In this way, we contribute to the theories developing in the field of IS security research.

References

Bagozzi, R, P., Yi, Y., and Phillips, L. W. (1991) "Assessing Construct Validity in Organizational Research", *Administrative Science Quarterly,* (36), pp. 421-458.

Berezina, K., Cobanoglu, C. Miller, B.L., & Kwansa, F.A. (2012) "The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth", *International Journal of Contemporary Hospitality Management*, Vol. 24 Iss: 7 pp. 991 – 1010.

Blakely, B. (2002) "Lock IT down: Consultants can offer remedies to lax SME security", *TechRepublic*, http://articles.techrepublic.com.com/5100-10878_11-1031090.html, Feb. 6, 2002.

Brown, C. V. and S. L. Magill (1994) "Alignment of the IS functions with the enterprise: Toward a model of antecedents." *MIS Quarterly*, 18(4), pp. 371.

Brown, C. V. and S. L. Magill (1998) "Reconceptualizing the context-design issue for the information systems function." *Organization Science*, 9(2), pp. 176-194.

Campbell, K., Gordon, L.A, Loeb, M.P., & Zhou, L. (2003) "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market", *Journal of Computer Security*, 11(3), pp. 431-448.

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004) "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", *Information Systems Research*, 16(1), pp. 28-47.

Chiasson, M.W. & Davidson, E. 2005 "Taking Industry Seriously in Information Systems Research", *MIS Quarterly*, 29(4), pp. 591-605.

Churchill, G, A. (1979) "A Paradigm for Developing Better Measures of Marketing Constructs", *Journal of Marketing Research* (16), pp. 64-73.

Cronbach, L. J. (1971). Test validation. In R. L. Thorndike (Ed.), *Educational measurement*, 2nd ed., Washington, DC: American Council on Education pp. 443-507.

Dimopoulos, V., Furnell, S., Jennex, M. & Kritharas, I. (2004) "Approaches to IT security in small and medium enterprises", *Second Australian Information Security Management Conference*, pp. 73-82.

Elliott, G. (2008) "The invisible Crime: A Business Crime Survey", *British Chamber of Commerce*, April.

Federal Aviation Administration. (2001) Executing The Risk Management Process, Nasdocs, URL http://nasdocs.faa.gov/nasiHTML/risk-mgmt/vol1/5_chapt.html

Garg, A., Curtis, J., & Halper, H. (2003) "Quantifying the Financial Impact of IT Security Breaches", *Information Management & Computer Security*, 11(2), pp. 74-83.

Gerbing, D. W., and Anderson, J. C. (1988) "An Updated Paradigm for Scale Development Incorporating Unidimensionality and Its Assessment", *Journal of Marketing Research* (25), pp. 186-192.

Goel, S. & Shawky, H.A. (2009) "Estimating the market impact of security breach announcements on firm values", *Information & Management*, (46), pp. 404-410.

Goodhue, Dale L., Straub, & Detmar W. (1991) "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security", *Information & Management*. Jan 20(1), p. 13-28.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. & Richardson, R. (2005) "CSI Computer crime and security survey", *Computer Security Institute* (10th Annual)

Herath, T., & Rao, R. (2009) "Protection motivation and deterrence: A framework for security policy compliance in organizations", *European Journal of Information Systems*, (18), pp. 106-125.

Hovav, A. & Gray, P. (2014) "The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis," *Communications of the Association for Information Systems*: (34), Article 50, pp. 893-912.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012) "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture", *Decision Sciences*, 43(4), pp. 615-659.

Keller et al., (2008), Information security breaches survey, PriceWaterHouseCoopers

Kankanhalli, Atreyi, Teo, Hock-Hai, Tan, Bernard C Y., Wei, Kwok-Kee, (2003) "An integrative study of information systems security effectiveness, *International Journal of Information Management*. Apr. 23(2), pp. 139-154.

King, J. (1983) "Centralized versus decentralized computing: Organizational considerations and management options." *Computing Surveys*, 15(4), pp. 319-349.

Rees, J., & Allen, J. (2008) "The state of risk assessment practices in information security: An exploratory investigation", *Journal of Organizational Computing and Electronic Commerce*, 18(4), pp. 255-277.

Richardson, R. (2008) CSI Computer crime and security survey, *Computer Security Institute, http://www.kwell.net/doc/FBI2008.pdf*

Richardson, R. (2010) CSI Computer crime security survey, *Computer Security Institute, http://gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2010.pdf*

Robins, G. (2001) Egovernment, Information Warfare, Risks Management: an Australian Case Study, *The Second Australian Information Warfare and Security Conference*.

Robinson, J. P., Shaver, P. R. & Wrightman, L. S. (1991) *Criteria for Scale Selection and Evaluation, in Measures of Personality and Social Psychological Attitudes*. San Diego, CA: Academic.

Sambamurthy, V. and R. W. Zmud (1999) "Arrangements for Information Technology Governance: A Theory of Multiple Contingencies," *MIS Quarterly*, 23(2), pp. 261-291.

Sindhuja, P.N. (2014) "Impact of Information Security Initiatives on Supply Chain Performance", *Information Management & Computer Security*, 22(5), pp. 450-473.

Slayton, R. (2015) "Measuring Risk: Computer Security Metrics, Automation, and Learning," *IEEE Annals of the History of Computing*, (15), pp. 32-45.

Straub, D.W. (1989) "Validating instruments in MIS research", *MIS Quarterly* 13(1), pp. 147-169.

Straub, D.W. (1990) "Effective IS security: An empirical study", *Information Systems Research*, 1(3), pp. 255-276.

NCC 2000. The Business Information Security Survey http://www.ncc.co.uk/.

Zafar, H., & Clark, J.G. (2009) "Current state of information security research in IS", *Communications of the Association of Information Systems, (*24), pp. 557-596l.